

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS**

JAMES EPPELEY, JENNIFER
MONILAW, and JACOB
WINKELVOSS, individually and on
behalf of all others similarly situated,

Plaintiffs,

v.

THE ALLSTATE CORPORATION,
ALLSTATE INSURANCE
COMPANY, ALLSTATE VEHICLE
AND PROPERTY INSURANCE
COMPANY, ARITY, LLC,
ARITY 875, LLC, and ARITY
SERVICES, LLC.,

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs James Eppley, Jennifer Monilaw, and Jacob Winkelvoss (“Plaintiffs”), by and through their undersigned counsel, file this Class Action Complaint (“Complaint”) against Defendants The Allstate Corporation, Allstate Insurance Company, Allstate Vehicle and Property Insurance Company (collectively, “Allstate Defendants”), and Defendants Arity LLC, Arity 875 LLC, and Arity Services LLC (collectively, “Arity Defendants”, and, with Allstate Defendants, “Defendants”), individually and on behalf of all others similarly situated, and in support thereof, allege as follows:

NATURE OF THE CASE

1. In recent years, insurance companies have pushed discounts to drivers if they provide access to telematics data gathered through mobile phone and vehicle systems as a solution to the steep rate increases drivers have experienced. Indeed, drivers have felt the pinch with the average cost of full coverage car insurance rising twenty-six percent in 2024 nationally.¹

2. Allstate Defendants are one such group of insurers who advertise discounts through their DriveWise program that includes a driver tracking app. However, unbeknownst to customers and the general public, the Allstate Defendants conspired with their subsidiary Arity Defendants to track customer and non-customer data far more broadly and invasively. Defendants provide auto insurance to 16 million customers, but Defendants purportedly built the “world’s largest driving behavior database,” housing the driving behavior of over 45 million Americans.² In fact, Defendants advertise that they have collected “trillions of miles” of consumers’ “driving behavior” data from mobile devices, in-car devices, and vehicles.³

¹ Shannon Martin, *The True Cost of Auto Insurance in 2024*, <https://www.bankrate.com/insurance/car/the-true-cost-of-auto-insurance-in-2024/> (last visited January 23, 2025).

² *Vehicle Miles Traveled*, ARITY, <https://arity.com/solutions/vehicle-miles-traveled/> (last visited January 23, 2025); and *Allstate: Everything You Need to Know*, INSURANCE BUSINESS, <https://www.insurancebusinessmag.com/us/companies/allstate/66989/> (last visited January 23, 2025).

³ ARITY-MAIN, <https://arity.com/> (last visited January 23, 2025)

3. Defendants harvested their “trillions of miles” of data not just when customers agreed to add the DriveWise program to their auto insurance policy, but through connections with consumers’ mobile devices created when consumers downloaded or used a myriad of apps on their phone. Defendants provided to app developers a software development kit, or SDK, that could be quickly integrated into their apps. When a consumer downloaded the third-party app onto their phone, they also unwittingly downloaded Defendants’ software. Once Defendants’ software was downloaded onto a consumer’s device, Defendants could monitor the consumer’s location and movement in real-time. Thus, as alleged herein, this database was built on the illicit collection of mobile phone geolocation data without providing meaningful notice, or eliciting informed consent, from their unsuspecting victims.

4. Through the software integrated into the third-party apps, Defendants pulled a variety of valuable data directly from consumers’ mobile phones, including a phone’s geolocation data, accelerometer data, magnetometer data, and gyroscopic data, which monitors details such as the phone’s altitude, longitude, latitude, bearing, GPS time, speed, and accuracy.

5. To encourage developers to adopt Defendants’ software, Defendants paid app developers millions of dollars to integrate Defendants’ software into their apps. Defendants further incentivized developer participation by creating generous

bonus incentives for increasing the size of their dataset. According to Defendants, the apps integrated with their software currently allow them to “capture[] [data] every 15 seconds or less” from “40 [million] active mobile connections.”

6. Once collected, Defendants found several ways to monetize the ill-gotten data, including by selling access to Defendants’ driving behavior database to other insurers and using the data for Allstate Defendants’ own insurance underwriting. If a consumer requested a car insurance quote or had to renew their coverage, insurers would access that consumer’s driving behavior in Defendants’ database. Insurers then used that consumer’s data to justify increasing their car insurance premiums, denying them coverage, or dropping them from coverage.

7. Defendants’ database goes far beyond supporting the Allstate Defendants’ car insurance business by, for instance, allowing Allstate Defendants to infer (correctly or incorrectly) driver behavior from geolocation data. Rather, Defendants profit from selling the driving behavior data to third parties, including other car insurance carriers, retailers, marketing companies, and any other party seeking to target their advertising to consumers based on their driving behavior.⁴ Millions of people were never informed about, nor consented to, Defendants’ continuous collection and sale of their data.

⁴ *Id.*

8. Defendants marketed and sold the data obtained through third-party apps as “driving” data reflecting consumers’ driving habits, despite the data being derived from and about the location of a person’s phone. More recently, however, Defendants have begun purchasing data about vehicles’ operation directly from car manufacturers. Defendants ostensibly did this to better account for their inability to distinguish whether a person was actually driving based on the location and movements of their phone. The manufacturers that Defendants purchased data from include Toyota, Lexus, Mazda, Chrysler, Dodge, Fiat, Jeep, Maserati, and Ram. Allstate Defendants have used this data for their own insurance underwriting purposes.

9. Consumers did not consent to, nor were aware of Defendants’ collection and sale of immeasurable amounts of their sensitive data. Pursuant to their agreements with app developers, Defendants had varying levels of control over the privacy disclosures and consent language that app developers presented and obtained from consumers. However, Defendants never informed consumers about their extensive data collection, nor did Defendants obtain consumers’ consent to engage in such data collection. Finally, Defendants never informed consumers about the myriad of ways Defendants would analyze, use, and monetize their sensitive data.

10. Defendants' conduct violates federal and state privacy laws, and prohibitions on unfair and deceptive acts and practices in the business of insurance.⁵

JURISDICTION AND VENUE

11. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this matter is brought as a class action pursuant to Fed. R. Civ. P. 23, the proposed Class includes more than 100 members, the Class contains at least one member of diverse citizenship from Defendant, and the aggregate amount in controversy exceeds five million dollars (\$5,000,000) excluding interest and costs.

12. The Court has personal jurisdiction over Defendants because Defendants maintain their principal places of business in this District, and Defendants have made sufficient contacts in this District, including the marketing and sale of insurance products.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendants are deemed to reside in this District, and a substantial part of the events, acts, and omissions giving rise to these claims occurred in this District.

⁵ See, e.g., *Concurring and Dissenting Statement of Commissioner Andrew N. Ferguson, In re Gravy Analytics, Inc. & In re Mobilewalla, Inc., Matter Nos. 2123035 & 2023196*, FEDERAL TRADE COMMISSION, (Dec. 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/gravy_-mobilewalla-ferguson-concurrence.pdf (“Given that the failure to obtain meaningful consent to the collection of precise location data is widespread, data brokers that purchase sensitive information cannot avoid liability by turning a blind eye to the strong possibility that consumers did not consent to its collection and sale. The sale of precise location data collected without the consumer’s consent poses a similarly unavoidable and substantial risk of injury to the consumer as does the sale of the non-anonymized data.”).

PARTIES

Plaintiff James Eppley

14. Plaintiff James Eppley is an adult citizen and resident of Conshohocken, Pennsylvania.

15. In or about 2020, Plaintiff Eppley downloaded certain third-party apps that integrated Defendants' SDK. Through Defendants' SDK, Defendants directly pulled a litany of valuable data directly from consumers' mobile phones. The data included a phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data, which monitors details such as the phone's altitude, longitude, latitude, bearing, GPS time, speed, and accuracy.

16. Plaintiff Eppley is informed and believes that his data, including location data, was provided to third parties, including, but not limited to, his auto insurance provider. This has led Plaintiff Eppley to pay more than he otherwise would have for his auto insurance.

Plaintiff Jennifer Monilaw

17. Plaintiff Jennifer Monilaw is an adult citizen and resident of Crystal Lake, Illinois.

18. In or about 2020, Plaintiff Monilaw downloaded certain third-party apps that integrated Defendants' SDK. Through Defendants' SDK, Defendants directly pulled a litany of valuable data directly from consumers' mobile phones.

The data included a phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data, which monitors details such as the phone's altitude, longitude, latitude, bearing, GPS time, speed, and accuracy.

19. Plaintiff Monilaw is informed and believes that her data, including location data, was provided to third parties, including, but not limited to, her auto insurance provider. This has led Plaintiff Monilaw to pay more than she otherwise would have for her auto insurance.

Plaintiff Jacob Winkelvoss

20. Plaintiff Jacob Winkelvoss is an adult citizen and resident of Wallingford, Pennsylvania.

21. In or about 2020 or 2021, Plaintiff Winkelvoss downloaded certain third-party apps that integrated Defendants' SDK. Through Defendants' SDK, Defendants directly pulled a litany of valuable data directly from consumers' mobile phones. The data included a phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data, which monitors details such as the phone's altitude, longitude, latitude, bearing, GPS time, speed, and accuracy.

22. Plaintiff Winkelvoss is informed and believes that his data, including location data, was provided to third parties, including, but not limited to, his auto insurance provider. This has led Plaintiff Winkelvoss to pay more than he otherwise would have for his auto insurance.

Defendant The Allstate Corporation

23. Defendant The Allstate Corporation is a United States public corporation headquartered in Glenview, Illinois, and incorporated under the laws of Illinois. Together with its subsidiaries, Defendant The Allstate Corporation provides insurance products, including car insurance, throughout the United States, including Illinois.

Defendant Allstate Insurance Company

24. Defendant Allstate Insurance Company is a wholly owned subsidiary of The Allstate Corporation and is headquartered in Northbrook, Illinois, and incorporated under the laws of Illinois. Defendant Allstate Insurance Company provides insurance products, including car insurance, throughout the United States, including Illinois.

Defendant Allstate Vehicle and Property Insurance Company

25. Defendant Allstate Vehicle and Property Insurance Company is a subsidiary of The Allstate Corporation and is headquartered in Northbrook, Illinois, and incorporated under the laws of Illinois. Defendant Allstate Vehicle and Property Insurance Company provides insurance products, including car insurance, throughout the United States, including Illinois.

Defendant Arity, LLC

26. Defendant Arity, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Chicago, Illinois, and it is incorporated under the laws of Delaware. Defendant Arity, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, including Illinois, and uses predictive analytics to build solutions to sell to third parties.

Defendant Arity 875, LLC

27. Defendant Arity 875, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Chicago, Illinois, and it is incorporated under the laws of Delaware. Defendant Arity 875, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, including Illinois, and uses predictive analytics to build solutions to sell to third parties.

Defendant Arity Services, LLC

28. Defendant Arity Services, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Chicago, Illinois, and it is incorporated under the laws of

Delaware. Defendant Arity Services, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, including Illinois.

FACTUAL ALLEGATIONS

A. Defendants Developed and Deployed the Arity SDK

29. In 2015 Allstate Defendants designed a software development kit (“SDK”) that could be integrated into mobile phone applications to collect data about the location and movements of a person's phone. SDKs can provide app developers a useful tool to build and develop their apps. Rather than independently develop code that will provide their app certain functionality, developers can use SDKs offered by third parties that will fill that role. SDKs usually consist of a set of tools (APIs, software, etc.) with preprogrammed functions that are integrated into an app and operate in the background. For example, one of the most common SDKs is Google Firebase which provides general-purpose user analytics to allow developers to optimize app performance.

30. But the SDK Defendants developed provided no such performance or development benefit. Rather, it was little more than a way for Defendants to scrape user data from third-party apps under the pretext of providing a necessary function. Specifically, Defendants designed the Arity Driving Engine SDK (“Arity SDK”)

to collect an immense amount of granular data points from or about the location of a person's mobile phone.

31. Once installed in a mobile app, the Arity SDK harvested several types of data, including but not limited to:

- a) a mobile phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data;
- b) "Trip attributes," which included information about a consumer's movements, such as start and end location, distance, duration, start and end time, and termination reason code;
- c) "GPS points," such as the accuracy, position, longitude, latitude, heading, speed, GPS time, time received, bearing, and altitude of a consumer's mobile phone;
- d) "Derived events," such as acceleration, speeding, distracted driving, crash detection, and attributes such as start and end location, start and end time, speed attribute, rate of change attribute, and signal strength attribute; and
- e) Metadata, such as ad ID, country code, iOS vs. Android indicator, User ID, device type, app version, and OS version.

32. Because the Arity SDK operated and collected data in the background, absent being notified by Defendants or the app, users would be kept in the dark about

the Arity SDK's existence. App users would likewise be unaware that Defendants were directly collecting Arity SDK data from their phones. Defendants never notified nor otherwise informed consumers that they were collecting their data via the Arity SDK and the apps.

B. Defendants Paid to Integrate the Arity SDK into Mobile Apps

33. Since at least 2017, Defendants have been "licensing" the Arity SDK by paying app developers millions of dollars to integrate the Arity SDK into their respective mobile apps. On information and belief, to avoid alerting consumers of their data collection, Defendants only sought to partner with apps that, prior to contracting with Defendants, already contained features that relied on location information to function properly. The apps that integrated the Arity SDK included MyRadar, Life360, and Fuel Rewards, which had, individually, more than 100 million downloads.

34. Each of these apps routinely requested and received permission from users to use their location information to enable certain in-app features prior to integrating the Arity SDK. For instance, GasBuddy, another popular app with more than 50 millions downloads, would access your location to find you the most affordable gas. But after an app integrated the Arity SDK, if an app user allowed the app to access their location information for those same in-app features, the user

was also unwittingly enabling Defendants to collect the mobile phone's geolocation via the Arity SDK.

35. Defendants' agreements with app developers generally had similar key provisions which allowed Defendants to use the Arity SDK to collect and use mobile phone data after the app developer integrated the Arity SDK into their mobile app. Pursuant to their agreements with the app developers, Defendants owned any data they collected from an app user and were permitted to use it for their own independent purposes. Defendants further agreed to license or transfer subsets of the data collected to the app developers to use for specific features in their apps, such as displaying a summary of a user's trip and fuel efficiency.

36. On information and belief, the Arity SDK Data in isolation could not (or at least could not reliably) be linked to a specific individual. To allow Defendants to match specific individuals to the data the Arity SDK collected, the app publishers licensed the personal data that they collected from their users to Defendants. The personal data that mobile apps licensed to Defendants generally included first and last name, phone number, address, zip code, mobile ad-ID ("MAID"), device ID, and ad-ID (collectively, "Personal Data"). Upon combining the Personal Data with the other collected location data, Defendants could more reliably identify the specific person being monitored by the Arity SDK.

C. Allstate Defendants Offer Drivewise

37. In 2010, Allstate Defendants began offering Drivewise®, which monitored driving behavior through a small telematics device provided by the company to customers at their request. Allstate Defendants offered that if customers installed Drivewise devices in their cars they could be rewarded for low mileage and safe driving by, for example, receiving lower rates or other discounts.⁶ In 2014, Allstate introduced Drivewise Mobile, the industry's first mobile telematics app.

38. The current iteration of the Drivewise program uses a mobile app that includes a “dashboard” providing driving feedback in real time, “driving insights” that provide personalized feedback on how users can make driving improvements, and a “trip summary” that includes trip histories, parking locations, and family driving insights.⁷

39. Drivewise identifies safe driving by automatically detecting when trips occur and collecting driving information such as speed, braking behaviors, and the time of day you're on the road.⁸

40. Nevertheless, Allstate Defendants recognize that “Drivewise follows the person, not the vehicle,” so the app will detect trips when you are a passenger in

⁶ *Our History*, ALLSTATE, <https://www.allstatecorporation.com/about/our-history.aspx> (last visited January 23, 2025).

⁷ *Drivewise from Allstate*, ALLSTATE, <https://www.allstate.com/drivewise> (last visited January 23, 2025).

⁸ *Id.*

a vehicle.⁹ Trips are assigned a predicted vehicle, i.e. automobile, train, bus, plane or boat, but can be wrong. The Drivewise user could also be identified as the driver when he or she is in fact the passenger. For this reason, and in clear recognition of the imperfect method that collecting driver trip data through a mobile phone represents, the Drivewise program allows users to edit recorded trips to correct mistakes before they are considered for any rate or discount decision.

41. Allstate Defendants include in the Drivewise app the Arity SDK, and through it share all data they collect through the app. Defendants clearly understand that no consumer would permit submission of driving data to their auto insurer without the opportunity to review and correct it. Allstate Defendants offer it with their own Drivewise app. Nevertheless, there is no such ability for any consumers to correct the data collected by the Arity Defendants through the Arity SDK, or how that information is further relayed to insurers.

D. Defendants' Products and Services Monetized Consumers' Data

42. Defendants used the data collected through the Arity SDK and the further provided Personal Data, alone and in conjunction with one another, to develop, advertise, and sell several different products and services to third parties, including insurers. Defendants' products and services included:

⁹ *Drivewise FAQs*, ALLSTATE, <https://www.allstate.com/drivewise/drivewise-faq-asc> (last visited January 23, 2025).

- a) Drivesight. In 2015, Allstate Defendants developed Drivesight to generate a driving score based on Defendants' own scoring model by analyzing data and generating driving scores that assign a particular value to an individual's driving risk.
- b) ArityIQ. Defendants let companies, including insurers, “[a]ccess actual driving behavior collected from mobile phones and connected vehicles to use at time of quote to more precisely price nearly any driver.”¹⁰
- c) Arity Audiences. Defendants let companies, including insurers, “[t]arget drivers based on risk, mileage, commuting habits” and “[m]ore effectively reach [their] ideal audiences with the best offers to eliminate wasted spend, increase retention, and achieve optimal customer LTV.”¹¹
As part of this product, Defendants displayed ads to the users of apps that agreed to integrate the Arity SDK.
- d) Real Time Insights. Defendants advertised that their business customers could “[r]eceive granular driver probe and event data for real-time applications.”¹²
- e) Routely. Defendants offer consumers Routely, a “free” application which purports to provide “helpful insights” into the consumers’ driver data. By

¹⁰ ArityIQ, ARITY, <https://arity.com/solutions/arity-iq/> (last visited January 23, 2025).

¹¹ Arity Audiences, ARITY, <https://arity.com/solutions/arity-audiences/> (last visited January 23, 2025).

¹² Real Time Insights, ARITY, <https://arity.com/solutions/real-time-insights/> (last visited January 23, 2025).

contrast, when marketing to insurers, Defendants describe Routely as “telematics in a box” that insurers can use to “more accurately identify drivers with riskier driving profiles based on actual driving data, provide personalized discounts or surcharges at renewal, promote safer driving habits, and improve retention of [their] safer drivers.”¹³

43. Notably, Defendants primarily marketed the Arity SDK data to third parties as “driving behavior” data as opposed to what the Arity SDK Data really was: data about the movements of a person’s mobile phone. On information and belief, Defendants had no way to reliably determine whether a person was driving at the time Defendants collected the Arity SDK Data.

44. For example, if a person was a passenger in a bus, a taxi, or in a friend’s car, and that vehicle’s driver sped, hard braked, or made a sharp turn, Defendants would conclude that the passenger, not the actual driver, engaged in “bad” driving behavior based on the Arity SDK data.¹⁴ Defendants would then subsequently sell and share the data so it could be used to inform decisions about that passenger’s insurability based on their “bad” driving behavior. Defendants’ public advertising for their products and services do not disclose the limitations of

¹³ *Routely*, ARITY, <https://arity.com/solutions/routely/> (last visited January 23, 2025).

¹⁴ As a further example, it was publicly reported that a person’s driving score was lowered because the “driving” behavior data collected from his phone claimed he was driving when he was actually riding a roller coaster. Chad Murphy, *Sir, This is a Roller Coaster. Car Insurance Dings Driving Score for Man Riding the Beast*, Cincinnati Enquirer, (Oct. 8, 2024), <https://www.cincinnati.com/story/entertainment/2024/10/08/insurance-cuts-driving-score-man-riding-the-beast-kings-island/75554987007/>.

the Arity SDK data. Defendants implicitly admit that their analysis can be flawed by allowing Allstate customers utilizing the Drivewise to go in and edit their trip record as described above.

45. Defendants sought to combine the Arity SDK data with other data collected directly from vehicles to address the inherent limitations of collecting cell phone location data. As a result, Defendants began purchasing consumers' driving-related data from car manufacturers, such as Toyota, Lexus, Mazda, Chrysler, Dodge, Fiat, Jeep, Maserati, and Ram. On information and belief, consumers did not consent, nor were otherwise aware that, Defendants purchased their driving-related data from these car manufacturers.

46. There are also additional issues related to pricing equities that using mobile phone location as a proxy for consumer behavior creates. For example, late-night driving is tracked and flagged as "high risk" by Defendants. However, low-income drivers working night-shift jobs are more likely to regularly drive during those "high risk" hours for commuting purposes rather than another late night social activity that implies riskier driving behavior.

47. Regardless, Defendants tout their ability to market and sell user data stating "[t]elematics data available at time of quote through the Arity IQSM network was exactly what many of our partners needed to return to a stable, profitable state." Defendants further attribute the industry's swing to a \$9.3 billion underwriting gain

in Q1 of 2024, compared to the \$8.5 billion loss in Q1 of 2023, to insurers' more widespread use of their telematics information.¹⁵

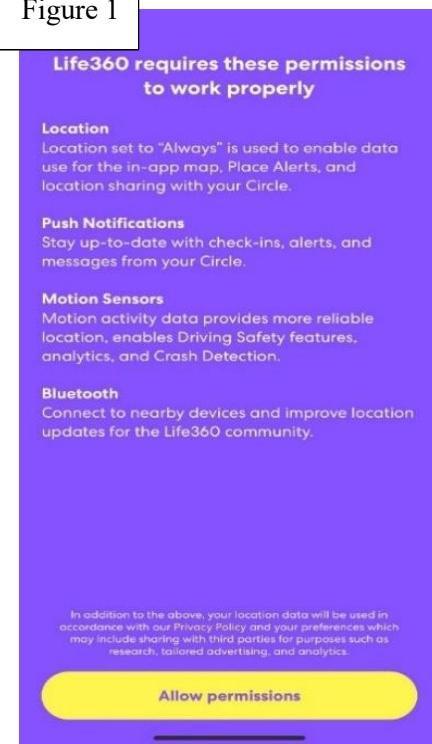
E. Defendants' Lack of Privacy Disclosures

48. Pursuant to their agreements with app developers, Defendants had varying levels of control over the privacy disclosures and consent language that app developers presented to consumers. However, neither Defendants, nor the apps on Defendants' behalf, adequately informed consumers that Defendants were collecting Arity SDK data, or of the various ways that Defendants would collect, use, and ultimately monetize the Arity SDK data, including by providing the Arity SDK data to Allstate Defendants or other insurers.

49. For example, Life360 merely told app users that it needed location sharing turned on “to enable data use for the in-app map, Place Alerts, and location sharing with [a user’s] Circle.” Nowhere did Life360 even mention Defendants’ existence, let alone any of Defendants’ data collection or sales.

¹⁵ Jen Gold, *How Telematics is Revolutionizing Auto Insurance Marketing Strategies*, ARITY (Oct. 21, 2024) <https://arity.com/move/how-telematics-is-revolutionizing-auto-insurance-marketing-strategies/>

Figure 1



50. Similarly, Fuel Rewards requests permission to track location to “Allow Fuel Rewards to use your location to help find the best gas prices near you and to send you personalized offers and location based alerts.” Nowhere is it disclosed that users’ mobile phone location data is being used to infer driving behavior for purposes of auto insurance underwriting, nor would any reasonable consumer infer that.

Figure 2



Location Services

Allow Fuel Rewards ® to use your location to help find the best gas prices near you and to send you personalized offers and location-based alerts. This information may be collected while you are using the app and in the background. We will also share or disclose your location with third parties, including our business partners as described in our privacy policy, to provide you with personalized offers.

Allow Location

51. Because Defendants did not disclose their conduct, consumers were wholly unaware that Defendants were collecting the Arity SDK data from their phone, the purpose of that collection, or Arity Defendant's relationship to Allstate Defendants. Consumers were likewise wholly unaware that Defendants would use the Arity SDK Data to create and sell several different products and services to third parties, including insurers.

52. Defendants did not provide consumers with any sort of notice of their data and privacy practices, nor did the mobile apps notify consumers about

Defendants' practices on Defendants' behalf. *See* Figure 1 and Figure 2. Similarly, neither Defendants nor the mobile apps notified consumers of the ways in which their Arity SDK data would be used, nor did consumers agree to have their data used for Defendants' own products or services. *See id.*

53. Even if a consumer took the extra step to investigate Defendants outside of their app, navigated to Defendants' website, and located their privacy disclosures, they would still not understand what Defendants did with their data or their relationship to the insurance industry. Consumers reading Defendants' privacy disclosures are met with a series of untrue and contradictory statements that do not reflect Defendants' practices.

54. For example, Defendants state that they "do not sell personal information for monetary value," which is untrue. Defendants sold a number of data-based products and services for monetary value that linked a specific app user to their alleged driving behavior. Further, Defendants do not provide consumers with the ability to request that Defendants stop selling their data. *See Exhibit A.*

55. Defendants likewise obscured how they used consumers' data. In Defendants' privacy disclosures, Defendants state that they "[u]se [consumers'] personal data for analytics and profiling." But in describing how Defendants "profile" consumers, the description does not reflect their actual "profiling" conduct—which consisted of Defendants combining the Arity SDK data and

Personal Data to create a database of driving profiles for more than 45 million Americans and selling access to said database. Rather, Defendants describe their profiling activities as follows:

“We use your personal data to assist in our development of predictive driving models. We may profile [consumers’] personal data only for the purposes of creating a driving score (“Driving Score”), which is used for our analytics purposes to develop and validate our predictive driving models.” *See Exhibit A.*

56. In the event a consumer took the extraordinary steps of tracking down Defendants’ privacy statement, finding the subparagraph describing profiling, parsing through Defendants’ convoluted description of their profiling activities, and concluding that they did not want Defendants to use their data to create a “Driving Score” about them, consumers still could do nothing to stop Defendants from collecting their data and creating a Driving Score. Defendants did not describe, nor provide, a method for a consumer to request that their data not be used to profile them.

57. Similarly, if a consumer concluded they did not want Defendants to use their data for targeted advertising, Defendants instructed them that they could “[l]earn how to opt out of targeted advertising” by visiting another link. But if a consumer followed that link, they would be taken to a page that--instead of offering

them a way to submit a request to opt out of targeted advertising--only provided them with links to several third-party websites, such as the Apple Support Center. These third-party websites merely contained explanations regarding how a consumer could turn off certain types of targeted advertising and did not contain a way for a consumer to submit a request to Defendants specifically.

58. As a result of Defendants' misconduct, Plaintiffs and the other Class Members were each injured on account of their location being shared with third parties, including, but not limited to, the insurance companies that provide them insurance and/or other insurance companies where Plaintiffs and the other Class Members applied for insurance.

59. To date, Plaintiffs' and Class Members' data is still in the possession of Defendants and unknown third parties. As such, and without the benefit of discovery, it is for all practical purposes impossible to know at this time whether a remedy at law or in equity will provide the appropriate full relief for Plaintiffs and the other Class Members. As a result, Plaintiffs, at this stage of the litigation, seek both restitution and a remedy at law, where the claims so permit. Further, Plaintiffs seek an injunction enjoining Defendants and their agents, servants, and employees, and all persons acting under, in concert with, or for them, from selling or otherwise disseminating Plaintiffs' and Class Members' data, and requiring that data's destruction.

TOLLING OF STATUTES OF LIMITATIONS

60. Defendants had exclusive knowledge of their activity to collect and utilize Plaintiffs' and Class Members' data and knew their activity would not be discovered by Plaintiffs and Class Members.

61. Thus, any applicable statute of limitations has been tolled by Defendants' actions and Defendants are estopped from pleading the statute of limitations because they failed to disclose the facts they were obligated to disclose concerning their activity.

CLASS ACTION ALLEGATIONS

62. Plaintiffs seek relief in their individual capacity and seek to represent a class consisting of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiffs seek certification of the following "Nationwide Class":

Nationwide Class

All persons residing in the United States whose mobile phone data was collected, distributed, stored, used, and/or sold by Defendants.

63. Plaintiffs Eppley and Winkelvoss seek to certify the following state class:

Pennsylvania Class

All persons residing in Pennsylvania whose mobile phone data was collected, distributed, stored, used, and/or sold by Defendants (the “Pennsylvania Class”).

64. Plaintiff Monilaw seeks to certify the following state class:

Illinois Class

All persons residing in Illinois whose mobile phone data was collected, distributed, stored, used, and/or sold by Defendants (the “Illinois Class”).

65. All Plaintiffs also seek certification of the following nationwide “FCRA Class”:

FCRA Class

All persons and entities in the United States whose vehicle driving data was included in consumer reports created and/or disseminated by Defendant Arity Services, LLC.

66. The Nationwide Class, the FCRA Class and the state classes above are collectively referred to herein as the “Class,” and their members as “Class Members.”

67. Plaintiffs reserve the right to amend or modify these Class definitions after they have had an opportunity to conduct discovery.

68. Numerosity. Fed. R. Civ. P. 23(a)(1). The Class is so numerous that joinder of all members is unfeasible and impracticable. While the precise number of

Class Members has not been determined at this time, Plaintiffs are informed and believe that millions of consumers had their location data collected and transmitted by Defendants.

69. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include for the Class, without limitation:

- a. Whether Defendants collected Plaintiffs' and Class Members' mobile phone data;
- b. Whether Plaintiffs and Class Members consented to such collection;
- c. Whether Defendants were unjustly enriched;
- d. Whether Defendants' conduct constitutes an invasion of privacy;
- e. Whether Defendants' conduct was knowing and willful;
- f. Whether Defendants are liable for damages, and the amount of such damages; and
- g. Whether Defendants should be enjoined from such conduct in the future.

70. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of the claims of Class Members. Plaintiffs and all Class Members were exposed to uniform

practices and sustained injury arising out of and caused by Defendants' unlawful conduct.

71. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

72. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

COUNT I
Violation of the Federal Wiretap Act
18 U.S.C. § 2510, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

73. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

74. The Federal Wiretap Act ("FWA"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.

75. In relevant part, the FWA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring "any other person to intercept

or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a).

76. The FWA also makes it unlawful for any person to intentionally disclose, or endeavor to disclose, to any other person or to intentionally use, or endeavor to use, the “contents of any wire, oral, or electronic communication, knowing or having reason to know that” the communication was obtained in violation of the FWA. 18 U.S.C. § 2511(1)(c) & (d).

77. The FWA provides a private right of action to any person whose wire, oral, or electronic communication is intercepted, used, or disclosed. 18 U.S.C. § 2520(a).

78. The FWA defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4).

79. The FWA defines “electronic communication” as “any transfer of signs, signals, . . . data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12).

80. The FWA defines “electronic, mechanical, or other device” as “any device or apparatus which can be used to intercept a wire, oral, or electronic communication.” 18 U.S.C. § 2510(5).

81. The FWA defines “contents,” with respect to any covered communication, to include “any information concerning the substance, purport, or meaning of that communication[.]” 18 U.S.C. § 2510(8).

82. The FWA defines “person” to include “any individual, partnership, association, joint stock company, trust, or corporation[.]” 18 U.S.C. § 2510(6).

83. Defendants, corporations, are each a person as defined by 18 U.S.C. § 2510(6).

84. As alleged herein, Defendants have intercepted, in real time and as they were transmitted, the contents of electronic communications, including but not limited to geolocation data, accelerometer data, magnetometer data, and gyroscopic data.

85. The data and transmissions within, to, and from Plaintiffs’ and Class Members’ phones constitute “electronic communications,” as defined by 18 U.S.C. § 2510(12), as they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic, or photooptical systems that affect interstate commerce.

86. Defendants intercepted these transmissions by collecting them via Defendants’ SDK to their own servers, unbeknownst to Plaintiffs and Class Members.

87. As detailed herein, the electronic communications detailed above that Defendants have intercepted are tied to individuals and not anonymized.

88. Plaintiffs and Class Members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant would violate state and federal privacy laws. Plaintiffs and Class Members were not aware and could not have reasonably expected that unknown third parties would install software on their mobile devices that would track and transmit their physical location and communications, and share Plaintiffs' and Class Members' personal information with other parties.

89. In further violation of the FWA, Defendants have intentionally used or endeavored to use the contents of the communications described above knowing or having reason to know that the information was obtained through interception in violation of 18 U.S.C. § 2511(1)(a) and 18 U.S.C. § 2511(1)(d).

90. Specifically, Defendants have used the contents of the communications described above to increase driving insurance premiums for members of the Class for their own financial and commercial benefit, obtaining substantial profit.

91. As a result, Plaintiffs and Class Members have suffered harm and injury due to the interception, disclosure, and/or use of communications containing their private and personal information.

92. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made by Defendants as a result of the violation or (b) statutory damages for each Class Member of whichever is the greater of \$100 per day per violation or \$10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

93. Plaintiffs and Class Members seek compensatory, injunctive, and equitable relief in an amount to be determined at trial, including an award of reasonable attorneys' fees and costs and punitive or exemplary damages for Defendants' willful violations.

COUNT II
Violation of the Stored Communications Act
18 U.S.C. §§ 2701, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

94. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

95. The Federal Stored Communications Act ("SCA"), enacted in 1986 as part of the Electronic Communications Privacy Act ("ECPA"), creates a civil remedy for those whose stored electronic communications have been obtained by

one who “intentionally accesses without authorization” or “intentionally exceeds an authorization to access” a facility through which an electronic communication service (“ECS”) is provided. 18 U.S.C. §§ 2701, 2707.

96. The Act reflects Congress’s judgment that users have a legitimate interest in the confidentiality and privacy of communications in electronic storage.

97. “Electronic communication” is defined as “any transfer of signs, signals, . . . data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12).

98. “Electronic communication service” means “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15) (incorporated by reference in 18 U.S.C. § 2711(1)).

99. “Electronic storage” is defined as “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication . . .” 18 U.S.C. §§ 2510(17) (incorporated by reference in 18 U.S.C. § 2711(1)).

100. Plaintiffs and Class members, as individuals, and Defendants, as corporations or legal entities, are “persons” within the meaning of 18 U.S.C. § 2510(6), and for purposes of 18 U.S.C. § 2707.

101. The data and transmissions within, to, and from Plaintiffs’ and Class Members’ phones constitute “electronic communications,” as defined by 18 U.S.C. § 2510(12), as they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic or photo optical systems that affect interstate commerce.

102. Plaintiffs’ and Class Members’ communications were intercepted by Defendants’ SDK, and stored on their own servers, unbeknownst to Plaintiffs and Class Members.

103. As detailed herein, the electronic communications detailed above that Defendants have intercepted are tied to individuals and not anonymized.

104. As alleged herein, there is a reasonable expectation of privacy within a person’s Electronic communications, and Plaintiffs and Class Members’ reasonably expected privacy while using their phones based on common understanding.

105. Plaintiffs and Class Members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant would violate state and federal privacy laws. Plaintiffs and Class

Members were not aware and could not have reasonably expected that unknown third parties would install software on their mobile devices that would track and transmit their physical location and communications, and share Plaintiffs' and Class Members' personal information with other parties.

106. Plaintiffs and Class Members did not authorize Defendants to access their phones or the communications stored within them.

107. Defendants intentionally accessed these communications without authorization.

108. In accessing Plaintiffs' and Class Member's phones and data without authorization and, in doing so, obtaining access to the electronic communications stored there, Defendants violated the SCA, 18 U.S.C. § 2701.

109. Defendants' conduct was willful and intentional, and invaded Plaintiffs' and Class Members' expectations of privacy within their phone and privacy of the personal interactions and communications.

110. Defendants have profited from their violation of the SCA, by, among other things, using the improperly accessed communications, location data and personal data to sell to third parties, and increase the price of car insurance.

111. The communications unlawfully accessed by Defendants have significant value, evidenced by the expenditures made by Defendants in order to deploy SDK's across applications and to collect information directly from vehicles.

112. Because of Defendants' conduct, Plaintiffs and Class Members have forever lost the value of their data, their privacy interest in the data, and their control over its use.

113. Because Plaintiffs and Class Members have been aggrieved by Defendants intentional acts in violation of the SCA, Plaintiffs and the Class are entitled to bring this civil action to recover relief and damages. 18 U.S.C. § 2707.

114. As a result of Defendants' conduct, Plaintiffs and Class Members are entitled to all damages set forth in 18 U.S.C. § 2707 including declaratory and equitable relief, compensatory damages measured by actual damages and Defendants' profits, reasonable attorneys' fees and costs, all available statutory relief, and punitive damages as determined by the Court.

COUNT III
Violation of the Computer Fraud and Abuse Act
18 U.S.C. § 1030, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

115. Plaintiffs re-allege and incorporate herein all foregoing factual allegations.

116. The Computer Fraud and Abuse Act ("CFAA"), enacted in 1986 as part of the ECPA, prohibits the intentional accessing, without authorization or in excess of authorization, of a computer under certain circumstances. 18 U.S.C. § 1030(a).

117. The Act reflects Congress' judgment that users have a legitimate interest in the confidentiality and privacy of information within their computers.

118. The CFAA specifically provides that it is unlawful to "intentionally access a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(c).

119. The CFAA also specifically provides that it is unlawful to "knowingly and with intent to defraud, access[] a protected computer without authorization or exceed[ing] authorized access" and thereby "further[] the intended fraud and obtain[] anything of value . . ." 18 U.S.C. § 1030(a)(4).

120. Plaintiffs and Defendants, as corporations or legal entities, are "persons" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(12).

121. A "computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(10).

122. "Exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain." 18 U.S.C. § 1030(e)(6).

123. A “protected computer” is defined as “a computer . . . which is used in or affecting interstate or foreign commerce or communication . . . , [or that] has moved in or otherwise affects interstate or foreign commerce.” 18 U.S.C. § 1030(e)(2)(B).

124. Plaintiffs’ and Class Members’ phones constitute a “computer” within the meaning of the CFAA. 18 U.S.C. § 1030(e)(1).

125. The phones of Plaintiffs’ and Class Members’ are used in and affect interstate and foreign commerce and constitute “protected computers” within the meaning of the CFAA. 18 U.S.C. § 1030(e)(2)(B).

126. Defendants intentionally accessed the protected computers in Plaintiffs’ and Class Members’ possession through the usage of SDKs without Plaintiffs’ or Class Members’ authorization, or in a manner that exceeded Plaintiffs’ and Class Members’ authorization, and obtained information therefrom in violation of the CFAA. 18 U.S.C. § 1030(a)(2)(C).

127. As alleged herein, Defendants’ conduct constituted a knowing intent to defraud Plaintiffs and Class Members of their valuable data and profit thereby. 18 U.S.C. §1030(a)(4).

128. Defendants’ use of MAIDs, IDFAs, IDFVs and its SDK constitutes the manner by which Defendants accessed Plaintiffs’ and Class Members’ communications while they are using their smartphones.

129. The value of the information Defendants obtained from the protected computers in Plaintiffs' and Class Members' possession exceeded \$5,000 in a one-year period, as evidenced by Defendants' significant profits from the disclosures of this information. 18 U.S.C. § 1030(a)(4).

130. Plaintiffs and Class Members have suffered harm and injury due to Defendants' unauthorized access to the communications containing their private and personal information.

131. A civil action for violation of the CFAA is proper if the conduct involves "loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value." Because the loss to Plaintiffs and Class Members during any one-year period within the relevant timeframe, including the loss of their privacy interest in and control over their location and driving behavior data, exceeded \$5,000 in the aggregate, Plaintiffs and the Class are entitled to bring this civil action and are entitled to economic damages, compensatory damages, injunctive, equitable, and all available statutory relief, as well as their reasonable attorney's fees and costs and other relief as permitted by the CFAA. 18 U.S.C. § 1030(g).

COUNT IV
Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Nationwide Class)

132. Plaintiffs re-allege and incorporate by reference the preceding paragraphs.

133. Plaintiffs and Class Members have reasonable expectations of privacy in their mobile phones, vehicles, and with their movements, generally. Plaintiffs' and Class Members' private affairs include their locations.

134. The reasonableness of such expectations of privacy is supported by Defendants' unique position to monitor Plaintiffs' and Class Members' behavior through their access to Plaintiffs' and Class Members' mobile phone location data through the inclusion of their SDK in certain apps unbeknownst to Plaintiffs. It is further supported by the surreptitious and non-intuitive nature of Defendants' tracking practices.

135. Defendants intentionally intruded on and into Plaintiffs' and Class Members' solitude, seclusion, or private affairs by intentionally collecting and transmitting information via the SDK installed in their mobile phones.

136. These intrusions are highly offensive to a reasonable person.

137. Plaintiffs and Class Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

138. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and Class Members.

139. As a result of Defendants' actions, Plaintiffs and Class Members seek damages and punitive damages in an amount to be determined at trial. Plaintiffs and Class Members seek punitive damages because Defendants' actions--which

were malicious, oppressive, and willful-were calculated to injure Plaintiffs and Class Members and were made in conscious disregard of Plaintiffs' and Class Members' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

COUNT V

Unjust Enrichment (Quasi -Contract Claim for Restitution and Disgorgement) or, Alternatively, Breach of Contract (On Behalf of Plaintiffs and the Nationwide Class)

140. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

141. Plaintiffs and Class Members unwittingly conferred a benefit upon Defendants.

142. Defendants took and retained valuable personal location information belonging to Plaintiffs and Class Members when they intentionally and comprehensively tracked their mobile phone locations and driving behaviors without their consent.

143. Defendants were enriched when they utilized Plaintiffs' and Class Members' location information, gathered without consent, for their own financial advantage to sell in raw form, or use to create reports or other analyses for sale, including, but not limited to, reports of Plaintiffs' and Class Members' driving behaviors for automobile insurers.

144. In exchange for Plaintiffs' and Class Members' loss of privacy and the financial benefits Defendants enjoyed as a result thereof, including, but not limited to, profits from the sale of the location data, and reports based on that location data, Plaintiffs and Class Members received nothing.

145. It would be inequitable for Defendants to retain the benefits they have unjustly received. Therefore, as a result of Defendants' actions, Plaintiffs and Class Members seek an order that Defendants disgorge the profits and other benefits they have unjustly obtained.

146. Alternatively, to the extent Defendants successfully assert that any terms of service from a binding contract that sufficiently defines the parties' rights regarding Defendants' use of Plaintiffs' and Class Members' location information, thereby rendering a claim for unjust enrichment unavailable (which Plaintiffs deny in the first instance), then Plaintiffs allege that Defendants' conduct constitutes a breach of any such binding contract, including, but not limited to, the covenant of good faith and fair dealing implied into every contract. Defendants did not adequately disclose prior to collecting or selling Plaintiffs' and Class Members' mobile phone location and driving behavior data that it would or could be sold to automobile insurance companies with whom Plaintiffs and Class Members had an ongoing, or prospective relationship. By virtue of Defendants' conduct as alleged herein, including the sale of Plaintiffs' and Class Members' location information

without adequate disclosure beforehand, Defendants breached the covenant of good faith and fair dealing implied into every contract, including any applicable terms of service.

COUNT VI

**Violation of the Fair Credit Reporting Act
(On Behalf of Plaintiffs and the FCRA Class against Arity Defendants)**

147. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

148. Arity Defendant are “consumer reporting agenc[ies],” as defined in 15 U.S.C. § 1681a(f).

149. As alleged in more detail above, Arity Defendants, LLC collected Plaintiffs’ driving data and incorporated into consumer reports, as defined in 15 U.S.C. § 1681a(d), which it disseminated to insurance companies and financial institutions.

150. As a consumer reporting agency, Arity Defendants are required to follow reasonable procedures “to assure maximum possible accuracy of the information concerning” individuals in consumer reports that it disseminates. 15 U.S.C. § 1681e(b).

151. Arity Defendants failed to maintain procedures to maintain maximum possible accuracy regarding Plaintiffs and FCRA Class Members’ driving data.

152. Upon information and belief, the uncontextualized, misleading, and personal driving information in the consumer reports disseminated by Arity Defendants harmed Plaintiffs, including by significantly raising their insurance premiums and/or resulting in the denial of coverage.

153. With certain exceptions not applicable here, under 15 U.S.C. § 1681b, Arity Defendants “may furnish a consumer report relating to any consumer . . . in connection with any credit or insurance transaction that is not initiated by the consumer only if . . . the consumer authorizes the agency to provide such reports to such person.”

154. Plaintiffs and FCRA Class Members did not authorize Arity Defendants to include driving data in consumer reports about them.

155. As a result of each and every willful violation of the FCRA, Plaintiffs are entitled to actual damages as the Court may allow under 15 U.S.C. § 1681n(a)(1); statutory damages under 15 U.S.C. § 1681n(a)(1); punitive damages as the Court may allow under 15 U.S.C. § 1681n(a)(2); and reasonable attorney’s fees and costs under 15 U.S.C. § 1681n(a)(3).

156. As a result of each and every negligent violation of the FCRA, Plaintiffs are entitled to actual damages as the Court may allow under 15 U.S.C. § 1681o(a)(1); and reasonable attorney’s fees and costs under 15 U.S.C. § 1681o(a)(2).

COUNT VII
Violation of the Illinois Consumer Fraud Act
and Deceptive Business Practices Act
(815 Ill. Comp. Stat. §505/1, *et seq.*)
(On Behalf of Plaintiff Monilaw and the Illinois Class)

157. Plaintiff Monilaw realleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

158. Plaintiff Monilaw brings this claim on behalf of herself and the Illinois Class against Defendants.

159. Defendants are each a “person” as defined in 815 Ill. Comp. Stat. §505/1(c).

160. Plaintiff Monilaw and the Illinois Class members are “consumers” as defined by 815 Ill. Comp. Stat. §505/1(e).

161. Defendants’ conduct as described here was in the conduct of “trade” or “commerce” as defined by 815 Ill. Comp. Stat. §505/1(f).

162. Defendants’ deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp Stat. §505/2 include: (a) knowingly and improperly storing, possessing, using, and/or procuring Plaintiff Monilaw’s and Illinois Class members’ geolocation and driving data from their mobile phones; (b) using that geolocation and driving data, and other personal data gathered from other sources, to impose increased insurance rates; and (c) selling and/or transmitting Plaintiff Monilaw’s and Illinois Class members’ data to third parties without their consent.

163. Defendants' deceptive acts, representations, and omissions were material because they were likely to deceive reasonable consumers about the collection and use of the data gathered by Defendants. Defendants actions were further in violation of Plaintiff Monilaw's and the Illinois Class members' privacy rights under Illinois and federal statutory and common law. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

164. Defendants acted intentionally, knowingly, and maliciously to violate Illinois' Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. §505/1, and recklessly disregarded Plaintiffs Monilaw's and Illinois Class members' rights.

165. As a direct and proximate result of Defendants' unfair, unlawful and deceptive acts and practices, Plaintiff Monilaw and Illinois Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including, but not limited to: the increase, or potential increase, to rates charged or quoted by insurers, and the loss of value of their location or driving data.

166. Plaintiff Monilaw and the Illinois Class members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution,

punitive damages, injunctive relief, reasonable attorneys' fees and costs, and any other just and proper relief available under 815 Ill. Comp. Stat. §505/1, et seq.

COUNT VIII
**Violation of Pennsylvania's Unfair Trade Practices
and Consumer Protection Law**
73 Pa. Stat., *et seq.*

(On Behalf of Plaintiffs Eppley and Winkelvoss and the Pennsylvania Class)

167. Plaintiffs Eppley and Winkelvoss reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

168. Plaintiffs Eppley and Winkelvoss bring this claim on behalf of themselves and the Pennsylvania Class against Defendants.

169. Defendants, Plaintiffs Eppley and Winkelvoss and the Pennsylvania Class members are each a "person" within the meaning of 73. Pa. Cons. Stat. § 201-2(2).

170. Defendants were and are engaged in "trade" or "commerce" within the meaning of 73 Pa. Cons. Stat. § 201-2(3).

171. The Pennsylvania Unfair Trade Practices and Consumer Protection Law ("Pennsylvania CPL") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce[.]" 73 Pa. Cons. Stat. § 201-3

172. Defendants' deceptive, unfair, and unlawful trade acts or practices, in violation of the Pennsylvania CPL include: (a) knowingly and improperly storing, possessing, using, and/or procuring Plaintiffs Eppley's and Winkelvoss' and

Pennsylvania Class members' geolocation and driving data from their mobile phones; (b) using that geolocation and driving data, and other personal data gathered from other sources, to impose increased insurance rates; and (c) selling and/or transmitting Plaintiffs Eppley's and Winkelvoss' and Pennsylvania Class members' data to third parties without their consent.

173. Defendants' deceptive acts, representations, and omissions were material because they were likely to deceive reasonable consumers about the collection and use of the data gathered by Defendants. Defendants actions were further in violation of Plaintiffs Eppley's and Winkelvoss' and the Pennsylvania Class members' privacy rights under Pennsylvania and federal statutory and common law. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

174. Pursuant to 73 Pa. Cons. Stat. § 201-9.2(a), Plaintiffs Eppley and Winkelvoss and Pennsylvania Class members seek an order enjoining the Defendants' unfair or deceptive acts or practices and awarding damages and any other just and proper relief available under the Pennsylvania CPL.

COUNT IX
Violation of Pennsylvania Wiretapping and
Electronic Surveillance Control Act
18 Pa. C.S. §§ 5701, *et seq.*
(On Behalf of Plaintiffs Eppley and Winklevoss and the Pennsylvania Class)

175. Plaintiffs Eppley and Winklevoss reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

176. Plaintiffs Eppley and Winklevoss bring this claim individually and on behalf of the members of the Pennsylvania Class against Defendants.

177. To establish liability under The Pennsylvania Wiretapping and Electronic Surveillance Control Act, Plaintiffs need only to establish that Defendant “procure[d] any other person to intercept [electronic] communication.” 18 Pa. C.S. § 5725.

178. “Electronic communication” is defined as ‘[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system.’ 18 Pa. C.S. § 5702 (emphasis added).

179. As alleged herein, the Defendants have intercepted, in real time and as they were transmitted, the contents of electronic communications, including but not limited to geolocation data, accelerometer data, magnetometer data, and gyroscopic data.

180. Defendants intercepted these transmissions by collecting them via Defendants' SDK to their own servers, unbeknownst to Plaintiffs Eppley and Winkelvoss and Pennsylvania Class members.

181. Plaintiffs Eppley's and Winkelvoss' and Pennsylvania Class members' electronic communications were intercepted in Pennsylvania, which is "the point at which the signals [i.e., Plaintiffs Eppley's and Winkelvoss' and the Pennsylvania Class's electronic communications] were routed to [Defendants'] servers." *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 132 (3d Cir. 2022).

182. Plaintiffs Eppley and Winkelvoss and Pennsylvania Class members did not consent to Defendants' actions in wiretapping their mobile phone. Nor did Plaintiffs Eppley and Winkelvoss or Pennsylvania Class members consent to Defendants' intentional access, interception, reading, learning, recording, and collecting of Plaintiffs Eppley's and Winkelvoss' and Pennsylvania Class members' electronic communications.

183. The violation of WESCA constitutes an invasion of privacy sufficient to confer Article III standing. *In re Facebook Internet Tracking Litigation*, 956 F.3d 589, 598-99 (9th Cir. 2020).

184. Plaintiffs Eppley and Winkelvoss and Pennsylvania Class members seek all relief available under 18 Pa. C.S. § 5725, including statutory damages of \$100 dollars per day for each day of violation or \$1,000, whichever is higher.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

- A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives, and appointing the undersigned counsel as Class Counsel;
- B. Enjoining Defendants, from continuing to engage in the unlawful acts, omissions, and practices described herein;
- C. Ordering Defendants to pay compensatory, exemplary, and/or statutory damages to Plaintiffs and Class Members in an amount to be proven at trial;
- D. Ordering Defendants to pay restitution to Plaintiffs and Class Members;
- E. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiffs and Class Members;
- F. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded, as allowed by law; and
- G. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiffs demand a trial by jury of all claims in this Complaint so triable.

Dated: January 23, 2024

Respectfully submitted,

/s/ Tina Wolfson

Tina Wolfson

twolfson@ahdootwolfson.com

Robert R. Ahoot

rahdoot@ahdootwolfson.com

Theodore W. Maya (*pro hac vice* to be filed)

tmaya@ahdootwolfson.com

Christopher E. Stiner (*pro hac vice* to be filed)

cstiner@ahdootwolfson.com

AHDOOT & WOLFSON, PC

2600 W. Olive Avenue, Suite 500

Burbank, California 91505

Tel: (310) 474-9111

Fax: (310) 474-8585

*Counsel for Plaintiffs and the
Putative Classes*